## REMARKS

Claims 1, 7-11, 17-20, 27-31 are pending in this application. Claims 27-31 are newly added by this amendment. Claims 21-26 are canceled without prejudice to comply with the Examiner's election requirement. Applicant preserves the right to represent these claims at a later date or in further proceedings.

Claim 1 has been amended to recite in part "said crypto engine configured to encrypt and authenticate transmitted data, said crypto engine further configured to decrypt and authenticate received data". This amendment is supported in various parts of the application as filed, such as in the following paragraphs:

> **[0021]** Coupled between the MAC 210 and the PHY 230 is a crypto device 220. The crypto device 220 is preferably configured to encrypt/authenticate the data packet 250 using DES, 3DES, MD5, SHA1, RC4, or AES, or other similar protocols.

> **[0024]** In the receiving device, the ciphered data packet 250 is received by the PHY 290 and provided to the crypto engine 280, where the data is decrypted/authenticated and provided to the MAC 270.

(Specification, para. 0021, 0024)

Claim 1 has also been amended to recite in part "said crypto engine further configured to store data and security information during transmission of data, said crypto engine further configured to resend said stored data without use of said MAC if said PHY detects a collision". This amendment is supported in various parts of the application as filed, e.g.:

**[0040]** In this embodiment, the encryption memory 345 may be employed to temporarily store the data and associated security information as the packet is transmitted. If a collision is detected, the stored information may be immediately reused and resent, without the need for the processor or MAC to resend the data, or to send new security information such as a security association.

(Specification, para. 0040)

Claim 11 has been amended similarly to claim 1 and is supported by at least the already indicated parts of the specification.

New claim 27 recites features of claim 1 with the additional limitation "wherein portions of said crypto engine are implemented by reconfiguring existing hardware components on said PHY". This is supported in the specification by, for example:

**[0032]** In a further embodiment, the crypto device 340 may be deployed using existing hardware already present in the PHY. It will be appreciated that by reusing existing hardware already present on the PHY to enable crypto features, significant real estate savings in the device may result.

**[0033]** It is contemplated that a wide array of PHY components may be reused when implementing the disclosed cryptographic features. For example, the crypto device may reuse the PHY's pin or interface layout, memory map, various elements of the state machine, logic gates, or even one or more of the above. Likewise, devices exist that contain multiple PHYs, such as an Octal PHY that contain 8 PHY interfaces. In these devices the reuse of pins and other elements that already exist in the PHY can reduce die and package size, thus making the devices less expensive to manufacture.

(Specification, para. 0032, 0033)

Claims 11 and 17-20 were rejected under 35 U.S.C. § 112, ¶ 2, as allegedly being indefinite. The Office Action states that the previously presented clause of claim 11 "wherein said MDIO/MDC interface is configured for controlling both the PHY and crypto engine means" is not supported by Fig. 6c. The Office Action further assumes for examination purposes that clause to read instead "wherein said MDIO/MDC interface is configured for controlling both the PHY logic and the security logic". In order to advance prosecution, claim 11 has been amended to comply with the reading assumed by the Office Action. The § 112 rejections of claim 11 and of dependent claims 17-20 are believed to be overcome by this amendment.

Claims 1, 7-11, and 17-20 stand rejected under 35 U.S.C. § 103 as allegedly obvious over what the Office Action calls "Applicant's admitted prior art (AAPA)", in view of Dhir et al. (U.S. Patent Pub. No. 2005/0084076), and further in view of Buer et al. (US 2004/0139313A1). These rejections are respectfully traversed.

However, in order to advance prosecution, all independent claims have been amended to yet more clearly distinguish from the cited art. In particular, the prior art does not teach or suggest features of claim 1 such as "said crypto engine further configured to store data and security information during transmission of data, said crypto engine further configured to resend said stored data without use of said MAC if said PHY detects a collision." None of the cited art alone or in combination teaches or suggests these features.

As best understood by Applicant, neither Buer nor AAPA discuss collisions or resending data. Hence Buer and AAP do not teach or suggest the claimed features. Applicants' attorneys have found only one instance in Dhir of the word "collision," as part of a standard protocol name:

> sufficient gates **307** are available for programming. It further should be appreciated that MAC layers for IEEE 802.11a and HiperLAN2 technologies are significantly different. The MAC layer used for IEEE 802.11a is a Carrier Sense Multiple Access protocol, more particularly a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), where the MAC layer for HiperLAN2 is Time Division Multiple Access (TDMA) protocol in conjunction with time division duplexing (TDD). Accordingly, MAC and baseband controller module **302** is programmed according to which technology platform is being employed.

(Dhir, para. 0043)

As the acronym expansion suggests, CSMA/CA focuses on "Collision Avoidance" rather than collision detection. Similarly, the TDMA protocol focuses on collision avoidance as well. Dhir makes no mention of detecting collisions or storing data to resend when a collision is detected. As a result, Dhir does not teach or suggest the claimed features. In fact, Dhir teaches away from the claimed features by disclosing collision avoidance rather than detection.

Consequently, none of the cited references alone or in combination teach or suggest the indicated features of claim 1. The 103 rejection of claim 1 is believed overcome. By similar argument, the 103 rejections of claim 11 and all dependent claims are believed overcome as well.

New claim 27 is believed allowable on independent grounds. Claim 27 recites the additional limitation "wherein portions of said crypto engine are implemented by reconfiguring existing hardware components on said PHY". None of the cited art alone or in combination teaches or suggests this feature.

As best understood by Applicant, neither Buer nor AAPA teaches or suggests reconfiguring hardware components of a PHY to implement a crypto engine. Dhir discloses reprogramming a portion of an FPGA to implement a MAC:

> protocol. For example, PHY **102** may conform to the HomePNA 2.0 specification while PHY **104** may confirm to the 10 Mbps Ethernet (IEEE 802.3) specification. It is observed that these two specifications define a MAC that is substantially the same. This observation is especially important in an implementation using field programmable gate array (FPGA). This is because FPGA allows a small portion of its programmable fabric to be changed without affecting the rest of the programmable fabric. This process is called "partial reconfiguration." An example of partial reconfiguration is disclosed in an application note published in June, 2000, by Xilinx, Inc., the assignee of the present invention, as "Correcting Single-Event Upsets Through Virtex Partial Configuration." As a result, the portion of MAC that is common to both specifications does not need to be changed after configuration. Only a small portion specific to each specification needs to be changed when integrated circuit **100** is switched from HomePNA to Ethernet. Alternatively,

(Dhir, para. 0031)

However, Dhir provides no teaching or suggestion of reprogramming PHY components to implement a crypto engine. In fact, Dhir teaches away from reprogramming PHY components when not implementing two MACs with similar operation:

> **[0039]** In this architecture, MAC components **204** and **206** have very little in common. Thus, the above-mentioned partial reconfiguration may not present many advantages in this case. Consequently, both MAC components are pre-installed in integrated circuit **200**.

(Dhir, para. 0039)

Therefore, Dhir does not teach or suggest the claimed feature. Consequently, it is respectfully submitted that none of the cited references alone or in combination teach or suggest the indicated features of claim 27. Claim 27 and its dependent claims are thus believed allowable on independent grounds.

## CONCLUSION

Applicants' attorney believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

The Commissioner is hereby authorized to charge any additional fees, including any extension fees, which may be required or credit any overpayment directly to the account of the undersigned, No. 504480 (Order No. CISCP584).

Respectfully submitted,
WEAVER AUSTIN VILLENEUVE & SAMPSON LLP

/Roger S. Sampson/

Roger S. Sampson
Reg. No. 44,314

P.O. Box 70250
Oakland, CA 94612-0250
510-663-1100